WHAT WE CLAIM IS:

1. A system for communicating over a network having a plurality of secured users utilizing multi-level network security devices and a plurality of unsecured users employing no network security devices, said system comprising:

an interface unit configured to send a message from a first user;

a first multi-level network security device configured to intercept said message from the first user; and

a host configured to discard said message if said message violates security parameters associated with said interface unit,

wherein in a first mode, the first multi-level network security device is configured to send said message to a second user, and

wherein in a second mode the multi-level network security device comprises an encryptor configured to encrypt said message and send said encrypted message to a second multi-level network security device, and wherein in said second mode the second multi-level network security device comprises a decryptor configured to decrypt the message and send said decrypted message from said second multi-level network security device to a third user selected from said plurality of secured users.

2. The system of Claim 1, further comprising a third multi-level network security device configured to intercept said encrypted message, validate a signature of said first multi-level network security interface, and send said encrypted message from said third multi-level network security interface to said second multi-level network security interface.

3. The system of Claim 1, wherein each multi-level network security device is configured to use association establishment messages for authenticating other multi-level network security interfaces.

4. The system of Claim 1, wherein each multi-level network security device is configured to use association establishment messages for exchanging security parameters between said multi-level network security interfaces.

5. A system for mixed enclave communications over a network having both secured and unsecured users, the system comprising:

a network security device configured to permit communication over the network between one of said secured users and one of said unsecured users, and further configured to dynamically determine whether a user initiating communication is one of said secured users or one of said unsecured users; and

a control module operationally coupled to said network security device, the control module being configured to control passage of information between said one of said secured users and said one of said unsecured users to secure information residing with said one of said secured users against transfer to said one of said unsecured users when not permissible.

6. The system of Claim 5, wherein the network security device is configured to examine Internet Protocol (IP) addresses for identifying the secured and unsecured users.

7. The system of Claim 5, wherein the network security device is configured to use association establishment messages for said secured users in authenticating each other.

8. The system of Claim 5, wherein the network security device is configured to use association establishment messages for the secured users exchanging security parameters.

9. The system of Claim 5, wherein the network security device comprises an encryptor configured to encrypt information residing with one of the secured users.

10. An apparatus for providing multi-level security in a computer network having a plurality of users and at least one relatively secure portion relative to at least one relatively unsecure portion of the network, the apparatus comprising:

a network security device configured to intercept a message transmitted between said at least one secure and said at least one unsecure portions of said network, and further configured to determine whether network security parameters will be violated by said intercepted message;

an encryptor configured to encrypt said intercepted message if said intercepted message:

will not violate said network security parameters,
originates from a secure portion of said network,
is destined for another secure portion of said network, and
will traverse an unsecure portion of said network; and

if said network security parameters will not be violated:

in a first mode, the network security device is configured to transmit said intercepted message; and,

in a second mode, the network security device is configured transmit said encrypted intercepted message.

11. The apparatus Claim 10, wherein the network security device is further configured to select the types of messages that are permissible.

12. The apparatus of Claim 10, wherein the network security device is further configured to examine Internet protocol (IP) addresses for identifying the source and destination of said message.

13. The apparatus of Claim 12, wherein the network security device is further configured to use association establishment messages for allowing those users which reside in said at least one secure portion of said network to authenticate other users residing in other secure portions of said network.

14. The apparatus of Claim 13, wherein said association establishment messages comprise security parameters.

15. The apparatus of Claim 13, further comprising a host configured to utilize a message intended to evoke a response from a destination user selected from said plurality of users and intended to receive said message to determine whether said destination user resides in the same portion of the network as a source user selected from said plurality which sent said message.

16. The apparatus of Claim 15, wherein said message intended to evoke a response from said destination user comprises a message which evokes a response only if said destination user and source user reside in the same portion of said network.

17. The apparatus of Claim 10, further comprising a waiting queue configured to queue passage of information.

18. The apparatus of Claim 10, wherein the network security device is configured to create an entry in an association table indicative of the source of a received message.

19. The apparatus of Claim 18, wherein the network security device is configured to compare the message destination's security level to that of the source of said intercepted message, so as to determine if said intercepted message may proceed.

20. The apparatus of Claim 19, wherein if the message destination's security level is higher than that of the source, the intercepted message is permissible to be released.

21. The apparatus of Claim 19, wherein if the message destination's security level is equivalent to that of the source, information transfers between the message source and destination.

22. The apparatus of Claim 19, wherein when the message destination's security level is lower than that of the source, the intercepted message is not permissible to be released, unless said message is predicted.

23. An apparatus for communicating over a network having a plurality of secured users utilizing multi-level network security devices and a plurality of unsecured users, the apparatus comprising:

a first network security device configured to control the transmission of a message from a first user to a second user, wherein in the event that either (a) the first user is a secured user and the second user is an unsecured user, or (b) the first user is an unsecured user and the second user is a secured user, the first network security device is configured to intercept a message sent by the first user, determine whether network security parameters will be breached by said message, and transmit said message to said second user if network security parameters will not be breached by said message, and

in the event that both the first and second users are secured users, the first network security device is configured to

intercept the message sent by the first user,

determine whether network security parameters will be breached by said message,

encrypt said message using if network security parameters will not be breached by transmission of said message,

transmit said encrypted message to a second network security device utilized by said second user if network security parameters will not be breached by transmission of said message, and

the second network security device is configured to decrypt said encrypted message and transmit said decrypted message to the second user if network security parameters will not be breached by transmission of said message.

24. The apparatus of Claim 23, wherein the first network security device is configured to compare the message destination's security level to that of the source of said intercepted message.

25. The apparatus of Claim 24, wherein:

when the message destination's security level is higher than that of the source, the intercepted message is permissible to be released;

when the message destination's security level is equivalent to that of the source, information transfers between the source and destination; and,

when the message destination's security level is lower than that of the source, the intercepted message is not permissible to be released, unless said message is predicted.